EP3432A1 (3)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2003 (23.01.2003)

PCT

(10) International Publication Number
WO 03/007538 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US02/23237

(22) International Filing Date: 10 July 2002 (10.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/305,120 12 July 2001 (12.07.2001) US
10/099,554 13 March 2002 (13.03.2002) US

(71) Applicant *(for all designated States except US)*: **ICONTROL TRANSACTIONS, INC.** [US/US]; 1999 South Bascom Avenue, Suite 700, Campell, CA 95008 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RUSSO, Anthony, P.** [US/US]; 58 W 75TH Street, #3A, New York, NY 10023 (US). **MCCOY, Peter, A.** [GB/US]; 1453 30th Avenue, Santa Cruz, CA 95062 (US). **ROESKE, Thorsten** [DE/DE]; Schieggstr. 8a, 81479 Munich (DE).

(74) Agents: **ANANIAN, R., Michael** et al.; Dorsey & Whitney LLP, 4 Embarcadero Center, Suite 3400, San Francisco, CA 94111 (US).

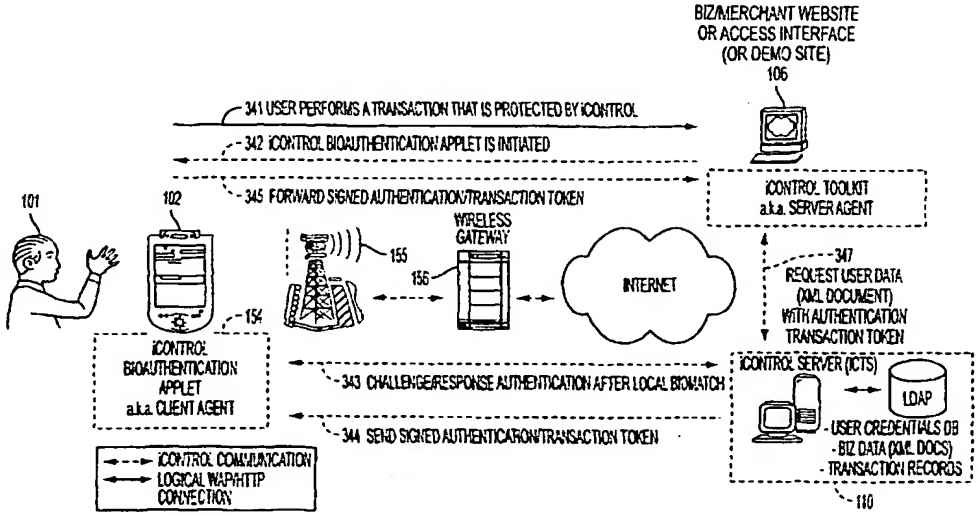
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) **Title:** OPERATING MODEL FOR MOBILE WIRELESS NETWORK BASED TRANSACTION AUTHENTICATION AND NON-REPUDIATION



(57) **Abstract:** An embodiment of the invention provides for a system, method, apparatus, and computer program product for device, user, and/or transaction verification, authentication, and non-repudiation. Wireless application (154) captures and utilizes biometric data (253, 279, 332) from user (101) in possession of mobile phone, PDA, or other portable computer (102). Information appliance (110) authenticates device (102) and/or user (101) to reduce or eliminate likelihood that transaction will be repudiated. Transaction authentication and non-repudiation (344, 356, 205) is applied to all manner of commerce including purchase and sale of products and services, banking, investment and other financial transactions (106), as well as in personal transaction not directly involving commerce. Authentication and non-repudiation occurs over a wireless or end-to-end wired network of interconnected computers (155, 103, 104).

WO 03/007538 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Operating Model for Mobile Wireless Network Based Transaction Authentication and Non-Repudiation

Inventors:

Anthony P. Russo

Peter A. McCoy

Thorsten Roeske

RELATED APPLICATIONS

Priority is claimed under 35 U.S.C. 120 and/or 35 U.S.C. 119(e) to United States Provisional Patent Application Serial No. 60/305,120 filed July 12, 2001 for *System, Method, Device And Computer Program For Non-Repudiated Wireless Transactions*; and to United States Utility Patent Application Serial No. 10/099,554 filed March 13, 2002 entitled *System, Method, And Operating Model For Mobile Wireless Network-Based Transaction Authentication And Non-Repudiation*, each of which is incorporated herein by reference.

Field of Invention

This invention pertains generally to device, user, and transaction verification and authentication systems and methods; and more particularly to device, user, and transaction verification, authentication, and non-repudiation system and method for mobile wireless applications that capture and utilize biometric data for transaction verification and authentication.

BACKGROUND

Heretofore, mobile Internet or other network-based transactions have been susceptible to security, identity fraud, and privacy risks. Stopping repudiation for a financial or other transactions on the basis that a person other than a person authorized to make the transaction actually made the transaction, have also presented significant concerns and costs to merchants and financial institutions. There has also been a desire to eliminate any need for entry of character based passwords on mobile device keypads, particularly where security requirements would impose characters in excess of a reasonable number of characters entered on such device keypad, such as for example eight character strings in order to provide to provide a desired security level. This is especially true for mobile telephones where there is a less than one-to-one ratio of keys to characters or numbers.

There has also been desirability of improving a user experience so that the user has confidence that's the transaction is being handled properly and in a professional manner without undue security risks. Improving the interface for the user, independent

of any added security, is also desirable so as to promote use of such mobile transaction systems.

In addition to or instead of Internet based mobile access, there is also desirability of providing protected access to content not otherwise publicly available with appropriate concern paid to controlling access to authorized parties in a manner that protects such non-public content (for example, private databases) or networks. For example, protected access to many intranet or extranet corporate database is desirable where a data center is desirable to support mobile professionals needing to retrieve information from, or communicate information to, such private databases, data systems, or networks.

Increasing the level of security to a level such that banks and other financial institutions that have or support credit card, debit card, or other financial instruments or transactions, have sufficient confidence in the access mechanism that they would be inclined to eliminate or reduce any customary "card not present" charges to online merchants, and even more desirably, to charge only the same rate for mobile Internet based transactions as charged when a physical card or other identification, authentication, or validation instrument is physically present is also highly desirable.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagrammatic illustration showing an embodiment of an infrastructure enabling secure mobile e-commerce using wireless BioPDA™ and having transaction non-repudiation features.

FIG. 2 is a diagrammatic illustration showing an embodiment of the interaction and communication flow in a wireless BioPDA™ implementation including authentication process.

FIG. 3 is a diagrammatic illustration showing an embodiment of an in-house intranet/extranet (non-Internet) implementation with optional remote Internet connectivity to the intranet/entranet.

FIG. 4 is a diagrammatic illustration showing an embodiment of an Internet based transaction authentication and non-repudiation service.

FIG. 5 is a diagrammatic illustration showing an embodiment of a wireless Password (PWD) Bank implementation.

FIG. 6 is a diagrammatic illustration showing an embodiment of the interaction and communication flow in a wireless Password (PWD) Bank implementation.

FIG. 7 is a diagrammatic illustration showing an embodiment of the data structure of an X.509 type ID certificate with exemplary private biometric extension (PBE).

FIG. 8 is a diagrammatic illustration showing an embodiment of the data structure for an exemplary Biometric Attribute Certificate (BAC) used in conjunction with an X.509 type Certificate.

FIG. 9 is a diagrammatic illustration showing an embodiment of a transaction token.

SUMMARY

Aspects of the invention provide system, method, apparatus, and computer program and computer program product pertaining generally to device, user, and transaction verification, authentication, and non-repudiation. It includes a mobile wireless application that captures and utilizes biometric data from a user in possession of a mobile phone, PDA, or other portable computer or information appliance that verifies the device and/or user so that the transaction may be verified and authenticated in a manner than substantially reduces or eliminates the likelihood that the transaction will be repudiated by the person to whom the transaction is attributed. Transaction authentication and non-repudiation features may advantageously be applied to all manner of commerce including the purchase and sale of products and services, banking, investment and other financial transactions, as well as in personal transaction not directly involving commerce in a conventional sense but where verification of identity is important.

In another aspect, the invention provides for authentication over a wireless network of interconnected computers or information appliances, such as the wireless Internet or a wireless device connected to the Internet. In another aspect, the invention provides end-to-end wired or wireless authentication infrastructure. In still another aspect, the invention provides a comprehensive network-based authentication system, method, device, and computer program and computer program product that provides non-repudiation for financial and other transactions on the mobile Internet or other network. In even still another aspect, the invention provides a business method and operating model for a transaction authentication and non-repudiation service.

In one embodiment, the invention provides a transaction authentication and non-repudiation system including a transaction server coupled with or intermittently coupleable to other information processing devices over a network, where the transaction server includes a database or is coupleable to a database storing at least one user credential and at least one transaction record, the transaction server including a processor and a memory coupled to the processor for executing transaction authentication instructions.

DETAILED DESCRIPTION

In one aspect, the invention provides system, method, apparatus, and computer program product pertaining generally to device, user, and transaction verification, authentication, and non-repudiation. It is particularly well suited for implementation as a mobile wireless application (or applications) that captures and utilizes biometric data from a user in possession of a mobile phone, PDA, or other portable computer or information appliance that verifies the device and/or user identity so that the transaction may be verified and authenticated in a manner than substantially reduces or eliminates the likelihood that the transaction will be repudiated by the person to whom the transaction is attributed. Such transaction non-repudiation feature is desirable for many types of commercial and financial transactions but is particularly useful for financial transaction, such as stock market or securities purchases or sales, where a user may be tempted to repudiate a buy or sell order to their financial advantage and to the detriment of the broker or financial institution performing the transaction on behalf of the user. Such transaction authentication and non-repudiation features may also clearly be

applied to all manner of commerce, including but not limited to the purchase and sale of products and services, as well as in personal transaction not directly involving commerce in a conventional sense but where verification of identity is important.

In another aspect, the invention provides for authentication over a wireless network of interconnected computers or information appliances, such as the wireless Internet. In another aspect, the invention provides end-to-end wired or wireless authentication infrastructure. In still another aspect, the invention provides a comprehensive network-based authentication system, method, device, and computer program and computer program product that provides non-repudiation for financial and other transactions on the mobile Internet.

Advantageously, in many of the inventive embodiments these and other inventive features and aspects are readily adapted to interoperate with existing device manufacturer's mobile telephone, Personal Data Assistants (PDAs), and computer products (such as for example, products made by Nokia, Ericsson, Acer, IBM, Palm, RIM, Handspring, Compaq), network operators (such as for example, Vodafone, NTT, Verizon, and AT&T), network platforms (such as for example, Phone.com, Inktomi, and Microsoft), and security providers (such as for example, Certicom, RSA, Verisign, Thawte, Baltimore, and Velocit-e). Furthermore, such features and aspects are also compatible with the needs and infrastructure of financial institutions (such as for example, Barclays Bank, VISA, Credit Lyonnaisse, and the like) as well as with Smart Cards/Wallets (such as smart cards and wallets made or supplied by G&D, Gemplus, Passport, and others). While compatibility and interoperability is advantageously maintained relative to many embodiments, it will be appreciated that other

embodiments of the invention may not provide compatibility with legacy systems as the technology evolves so as to provide advanced features.

In a preferred embodiment of the invention, system capabilities are extended using fingerprint bio-certification technology. In one embodiment, a standard X.509 certification is used. In another embodiment, a higher grade extended X.509 certification having biometric attributes is provided (referred to here as a BioCert). In other embodiments, information analogous to that provided with an X.509 type certificate is provided but the X.509 certificate itself is not required. Any of these certifications, but particularly the enhanced certification having biometric attributes, will (or are expected to) enable merchants to qualifying for reduced "card present" transaction rates from the card issuing organization for credit card, debit card, and the like transactions. The system method of the present invention therefore provide a number of improvements and capabilities beyond those presently available for mobile transactions. In one aspect, the invention provides an improved user experience. In another aspect, the invention provides biometric extensions to standard certificate infrastructure, and in particular biometric extensions to standard X.509v3 certificate infrastructure, as well as new certificate infrastructure incorporating biometric data. In yet another aspect the invention is biometric agnostic. In a further aspect, inventive system and method build on an expanded existing Public Key Infrastructure (PKI). In still another aspect, the inventive system and method provide for small or thin client side component footprints that interoperate and otherwise satisfying memory and processing limitations imposed by mobile phones, PDAs, and other typically thin mobile information appliances. In a further aspect, embodiments of the invention

provide optimized authentication and electronic signing (eSigning) protocols that work fast and reliably even over typically slow or limited connections available with wireless technologies. In yet another aspect, the invention provides extendable storage of user data, such as through the use of XML and/or extensions thereof, including but not limited to for example, extendable storage for a user's stock portfolio, or the like information. In yet a further aspect, the system and method provide for scalability and support for LDAP and UNIX-based Web servers, such as for example Apache, or the like.

Having now described some features and advantageous aspects of the invention, attention is now directed to a description of particular exemplary system configurations and methodological procedures which assist in understanding the manner in which the invention may be deployed and used.

Overview of Embodiment of System Infrastructure

An overview of one embodiment of the inventive system is now described relative to FIG. 1. An access device, preferably a hand-held device or portable device 102, such as a mobile phone, smartphone, personal data assistant (PDA), hybrid device such as an information appliance or portable computer/communication device having wireless communication capability is connected or intermittently connectable to a network 104 of computers or other information processing devices or appliances, such as the Internet. The network 104 may for example be, but is not limited to a network supporting communication using WML, HTML, CHTML, xHTML, or combination, variant, or extension thereof. Furthermore, while wireless communication takes

advantage of the features of the invention and provides a particularly advantageous operation, it will be appreciated that the invention is also operable with wired communication infrastructure.

In an exemplary configuration, the portable device 102 comprises a wireless BioPDA, where communication is achieved using radio-frequency communication techniques such as are well known in the art. In this embodiment, described relative to FIG. 1, a Compaq iPaq PDA running the Microsoft Pocket PC operating system (for example the iPaq H3600 series running Pocket PC version 3.0 or 2002) with a wireless modem (as are known in the art) is used as the base user device platform within portable mobile device 102. A PDA 102, such as the iPaq Pocket PC (for example, model H3600), palm, Sony Clie™, or handspring devices represent one type of mobile device 102. A fingerprint sensor, scanner, or other biometric capture device 151 is provided as an add-on component. Alternatively, a sensor scanner or other biometric capture device 151 may be provided internal to device 102 and be exposed through a surface or aperture on the surface of the device. For example, the compact flash adapter or PC card adapter with its ability to mechanically and electronically attach to and couple with the iPaq device 102 via a slot and connection may be used to attach the fingerprint sensor component. An add-on peripheral may similarly be attached to a communication infrastructure on a mobile phone. Client Agent Applet 152 for the Windows CE or Packet PC Browser (such as GoWeb from GoAmerica, Microsoft Explorer, or Microsoft MobileBrowser) and driver or drivers are also provided. Compatible browsers for the Palm Operating System (PALM OS), Linux, or other platforms may alternatively be provided. An inventive Client Agent Applet 152 or application

program is also used and may advantageously use a X.509v3 based certificate, such as the X.509v3 certificate with private "bio" extensions (PBE).

An embodiment of such a wireless biometric enabled PDA (BioPDA™) 102 uses a biometric sensor 151 (such as for example, a fingerprint sensor, a retinal scan sensor, a voice- or speech-based sensor, or any other biometric sensor), and computer code software/firmware Bioauthentication Applet 152 operative with the biometric sensor in the device 102. Note that the Compaq iPaq H3600 series devices (such as for example, the H3635, H3650, H3660, H3670, or H3700 or H3800 series) includes a microphone and voice recording capability that may be used where the biometric is or includes a voice or speech biometric identification or recognition parameter. Device 102 includes a wireless modem as an integral component or as an add-on device (such as a compact flash or PC card based wireless modem), or wireless telephone coupled to the PDA via serial, infrared (IRDA), or other communication or coupling means. Various wireless communication technologies including modem based communications for cellular telephones, PDAs, and mobile communication are known in the art and therefore are not described in greater detail herein.

With further reference to FIG. 1, BioPDA™ 102 communicates with a wireless receiver station 155, which in turn communicates to a wireless Internet gateway 156 via available wired or wireless communication channels or other means 103, which may, for example, comprise any conventional telephone line, satellite link, cable, wire or the like, as are known in the art. In some embodiments, wireless receiver station 155 and wireless Internet Gateway 156 are combined. Wireless Internet gateway 156 in turn couples to the Transaction Server (TS) 110 via Internet 104. Some portions of this

description refer to an "IControl" version or embodiment of an aspect of the invention. Such "IControl" references are made relative to certain commercial developments and design prototypes being undertaken by IControl Transactions, Inc., the Assignee of this invention. For example, reference is made to an IControl Transaction Server (ICTS) which is a particular embodiment of the Transaction Server (TS) 110. The wireless BioPDA system configuration of FIG. 1 also includes or inter-operates with a Business/Merchant Web Server (Biz/Merchant) BWS 106. A Server Agent (e.g. IControl Server Agent) 107 is advantageously provided with BWS 106, and desirably includes a Server Agent Toolkit (SAT) 109 to facilitate integration, testing, and maintenance. The Server Agent 107 and Server Agent Toolkit 109 are described in further detail elsewhere in this specification.

A demonstration web server site may optionally be provided (shown in some embodiments) to simulate an on-line business web server, such as for example an on-line stock trader. In such demonstration configurations, the particular Web application (such as a demonstration online stock trader) will not necessarily be part of the actual system.

In practice, an entity desirous of setting up and interfacing their web server with the inventive system and method, uses features, capabilities, and software provided with the Server Agent Toolkit 109. The inventive Transaction Server (TS or ICTS) and Server Agent Toolkit (SAT) are provided to a business, merchant, organization, individual, or other entity so that an authentication and non-repudiation compatible website may be constructed and interoperate with other inventive system components and methodological procedures. The Business Website server (or demonstration site)

106 is coupled to the transaction server 110 and wireless Internet gateway 156 via Internet 104.

Direct or other non-Internet connection may alternatively be provided or the BWS 106 may be co-located with the transaction server 110. In one embodiment, the business web site server 106 is or includes a demonstration site that replaces a real merchant§s website in actual system implementations, however, this is not the typical configuration. The transaction server such as ICTS 110 advantageously includes or is coupled to a database or databases, such as the LDAP databases 113, 114, storing user credentials, business data (such as XML documents or documents or data in other form), and transaction records.

A business or merchant computer configured as a Web server 106 is also connectable over a communication link or channel 103 to the Internet 104 as well as optionally to financial/banking/credit card infrastructure or organization 108. This latter connection to the infrastructure or organization 108 may be made by an Internet connection or by other shared or dedicated communication link, such as for example, a direct analog telephone connection, dedicated phone line, satellite, cable or the like. Characteristics of business or merchant Web server 106 are generally conventional in nature except for the components provided to Internet with the transaction server, and as numerous server configurations are known in the art, are not described here in greater detail.

An additional server, such as an Internet Web Server configured as the Transaction Server 110 when the network is the Internet, configured to provide at least some of the desired security and authentication features is also connected or connectable

to device 102 and Web server 106 via Internet 104. In one embodiment, this additional server 110 is referred to as the Internet Web Server (IWS) as a more specific Input implementation of a transaction server. It is noted that although multiple servers are described in which different aspects of the transaction take place on different servers, such logically diverse or geographically diverse processing is not required in all embodiments, and that many of the functions and/or operations may be processed in fewer servers or even in a single server in other embodiments.

Transaction server 110 includes a computer of conventional type having a processor or CPU, a memory coupled to processor for storing instructions and data during execution of computer programs, mass storage device such as a hard disk drive, and other input/output and peripheral components that support the data, content, and security or certificate transactions provided by server 110. In addition to these conventional components, server 110 advantageously includes one or more database or other storage devices or subsystems storing data using Lightweight Directory Access Protocol (LDAP) 113, 114.

The Client side components include a client agent 154 (in one embodiment, referred to as the IControl Client Agent) that comprises a software application (such as for example a computer program software or firmware application written in C, C++, Java, or any other application programming language suitable for a particular device or devices). Code or program libraries that operate on the user§s mobile device (for example, PDA, mobile phone, Smartphone, or other intelligent mobile information appliance) may also typically be utilized.

The functionality provided by any particular client agent 154 may sometimes be

dependent upon the particular client characteristics, however, it may generally provide at least some and in at least one embodiment of the invention, all of the following functions, some of which functions are optional but advantageously provided: (i) local (on client device) biometric authentication, (ii) support server-based biometric authentication, (iii) local digital transaction signing, (iv) Local audit-trails and logging, (v) client components for server based notarization, (vi) client components for server based audit-trails and logging capabilities, and (vii) local biometric authentication for access control to users PKI private keys. Each of these client agent based functions is now described in greater detail.

Client agent 154 provides local (that is on user client device 102) biometric authentication of a user (or of an attempted user) against a local database of users and their biometric samples or against a local database of Biocertificates. Such an authentication may for example be initiated by a Web Server or Web application, such as by BWS 106, in order verify the identity of a user and/or device attempting access to allow access to a protected resource on that Web Server.

Client agent 154 may also provide the necessary client components for server based biometric authentication of a user against a server side database of users and their biometric samples or against a server side database of Biocertificates. Such an authentication may also or alternatively be initiated by a Web Server or Web application in order verify the identity of a user to allow access to a protected resource on this Web Server.

Client agent 154 may further provide local digital signing of transactions, documents or other forms of electronic data involving biometric authentication of the

signer (which may be server based or local based), the signer§s Biocertificate(s) and/or private key(s). This may be based on RSA, elliptic curve or other techniques known in the art.

Client agent 154 may in addition provide local audit-trails and/or logging capabilities of performed biometric authentications and digital signatures such as my be useful in order to provide non-repudiation or documentary evidence to support non-repudiation, such as may be desired during a post-transaction legal proceeding.

Client agent 154 may yet further provide any necessary or desired client components for server-based notarization of a local digital signature (as described above) or biometric authentication.

Client agent 154 may further any necessary client components for server based audit-trails and logging capabilities of performed biometric authentications and digital signatures in order to provide non-repudiation or documentary evidence to support non-repudiation such as may be desired during a post-transaction legal proceeding.

Finally, client agent 154 may provide local biometric authentication for access control to users PKI private keys stored on the client device.

With further reference to **FIG.** 1, attention to some characteristics of an exemplary Transaction Server (TS) 110 such as the ICTS 110 or other Internet Web Server (IWS) configured as a transaction server. In one aspect, the transaction server may be considered to be one or more software application program(s) that reside on a computer web server and provides the server side capabilities for authentication services, digital signing services, archiving services, and/or other transaction non-repudiation services. It can be physically and logically located within the customer§s

premise, behind a firewall of the customer (such as for example, where the merchants web server resides) or it can be hosted by a trusted or otherwise independent third party (such as for example, a network operator, bank, system integrator, or the like) and used as a transaction non-repudiation application service provider (ASP). Depending on the particular implementation, the transaction server and transaction server application program(s) provides one or any combination of the following functions: (i) server based biometric authentication of a user, (ii) server based notarization of a client side digital signature, (iii) server based audit-trails and logging, (iv) interface to certificate authorities for enrollment of new users, and (v) interface to certificate authorities and certificate revocation lists for biometric authentication. Each of these transaction server based functions is now described in greater detail.

The transaction server application program or programs (recall that the transaction functions may be provided by possibly geographically diverse computer systems or components) provides any necessary server components for server based biometric authentication of a user against a server-side database of users and their biometric samples or against a server-side database of Biocertificates. Such an authentication might be initiated by a Web Server or Web application in order verify the identity of a user to allow access to a protected resource on this Web Server.

The transaction server 110 may also provide any necessary server components for server based notarization of a client side digital signature (see above) or biometric authentication. It may also provide any necessary server components for server based audit-trails and logging capabilities of performed biometric authentications and digital signatures in order to provide non-repudiation.

The transaction server application program may also provide an interface to one or more Certificate Authorities in order to generate a user§s Biocertificate in support of the enrollment of new users. It may further provide interface to one or more Certificate Authorities an/or certificate revocation lists to provide up-to-date information on the validity, revocation status, or other information regarding a used Biocertificate if it is based on a X.509 certificates, thereby supporting biometric authentication.

Finally, the third major component is the business or merchants web server (Biz/merchant web server) 106 including server agent 107, where business or merchant refers to a broad class of entities providing, retail or wholesale goods and/or services independent of whether such goods or services are provided free or for a fee, and including all financial, banking, brokerage, information, sales, decision, proxy, or the like goods and services.

In one embodiment, the web server includes a toolkit (also referred to as a software development kit or SDK) that provides any necessary applets and libraries for the integration of the mobile wireless network-based transaction and non-repudiation services (such as the authentication, transaction signing, non-repudiation services) into Web Sites or Web applications. Depending on the implementation, the server agent 107 provides one or any combination of following functions: (i) an interface between the mobile wireless network-based transaction and non-repudiation services and the application requiring such services, and (ii) a routing interface that provides a communication relay between the client agent 154 and the transaction server 110.

Addressing each of these server agent functions in further detail, the server agent 107 provides the interface between the mobile wireless network-based transaction

and non-repudiation services and the application (for example, the Web Site, Web Application or other applications) requiring such services. This interface may be implemented as function calls to libraries provided, rule-based Web (http) proxies that trigger functionality based on the analyses of passing messages/packets, embedded objects in html pages (such as ActiveX or Java Servelets), as ISAPI or NSAPI filters, as code in active server (ASP) or dynamic HTML pages, as Java applications, or in other ways as are known in the art. This interface provides the functionality for the integration of enrollment and maintenance of users, local or server side biometric authentication, and logging and auditing as well as digital biometric signing into the application requiring of such services. The application requiring such services can also define parameters for invoked function: for example, required authentication method (e.g. what type(s) of biometric technology such as fingerprint, voice, face, signature, or the like should be used), required score or degree of match of the used authentication methods, and/or required enrollment method, and the like.

The server agent "routing" interface provides a communication relay between the client agent and the transaction server. In one embodiment, all communication between the client agent 154 and the transaction server is routed through the server agent 107. In another implementation the client agent 154 communicates directly with the transaction server 110. In yet another embodiment the client agent 154 communicates directly as well as through the routing interface of the Server Agent 107 with the transaction server 110.

Note therefore that in at least one embodiment of the inventive system and method, in order to perform biometric authentication (local or server side) or digital biometric

signing (local or server side) including server side notarization, the client agent 154 has to communicate with the transaction server 110. In one implementation the client agent communicates directly with the transaction server, while in an alternative embodiment, the communication between client agent and transaction server flows through a relay function of the Server Agent 107. These communication methods and pathways are described in greater detail elsewhere in this description.

With reference to the embodiment illustrated in FIG. 2, aspects of communications that occur among and between system components and process as well as between system components and processes and external ones are now described. In a first embodiment, illustrated in FIG. 2A, the client agent communicates directly with the transaction server (that is without an intervening server agent). In a second or alternative embodiment, illustrated in FIG. 2B, the communication between the client agent and the transaction server flows through a relay function of a server agent 107. Each of these alternative embodiments are now further described relative to the figures. Either of these configurations may further involve data, information, tokens, packets, or the like flowing through third party or other intermediate servers as one known in the Internet arts. In each of these diagrams, dashed or broken lines identify an IControl Communication ("control communication") while solid or un-broken lines identify logical WAP/HTTP connections ("logical connection"), typically built upon an underlying TCP/IP protocol.

With reference to FIG. 2A, in this communication flow, a user first performs a transaction over a logical connection that is protected by the inventive method (such as the IControl method) thereby causing a communication between the client agent 102

(such as the bioauthentication applet) executing on the client device and business/merchant server agent 106 executing on the business/merchant web server (Step 341). Note that this communication normally occurs over a logical WAP/HTTP connection as indicated by the solid line in the drawing. Next, the bioauthentication applet on the client device is initiated (Step 342) by the server agent, such that a biometric sample is collected by the client device (such as a fingerprint sample) and compared against stored authorized biometric indicia resulting in a local match or local non-match. This communication normally occurs as a system (e.g. IControl) communication as indicated by the broken or dashed line in the drawing. A first non-match may result in a predetermined number of retries. A bi-directional challenge/response authentication after local match is performed between the client agent and the transaction server (Step 343). If the authentication is successful, the transaction server sends a signed authentication/transaction token to the client agent (Step 344). The client agent then forwards the signed authentication/transaction token to the server agent on the business/merchant web site (Step 345). The Server agent and the transaction server communicate via request and response to exchange user data (such as in the form of an XML document) with authentication/transaction token (Step 347). Note that in one embodiment, the transaction server includes a LDAP-based database including user credential data such as business data in the form of XML or other documents or data and transaction records.

With reference to FIG. 2B, similar functionality is provided, however, the communication between the client agent and the transaction server flows through a relay function of a server agent. In this embodiment, optionally, a SSL/TLS session is

established (Step 351). Next, but also optionally, user authentication is performed bi-directionally based on the inventive IControl Non-Repudiation Infrastructure (ICNRI) according to the servers security policy (Step 352). These first two steps are optional and are not required in all embodiments, for example, they are not required where communication between the client agent and the business/merchant web server is already present or provided by other means.

The user then requests a transaction protected by the inventive method, usually according to security policy (Step 353). The client agent program applet is initiated and is downloaded prior to initiation if not already present on the client device (Step 354). A bi-directional challenge/response authentication procedure is performed between the client agent and the transaction server via the server agent applet (that is indirectly) after local biometric match is performed on the client (Step 355). Note that this step involves a communication between the server agent and the transaction server to relay the challenge/response (C/R) from the client agent to the transaction server (ICTS). This step (Step 355) therefore includes a client agent to server agent component (step 355a) and a server agent to transaction server component (step 355b). A copy of the signed Authentication/transaction token is forwarded to the client agent (Step 356), first from the transaction server sending a signed authentication/transaction token to the business/merchant web site server (step 356a), and the business/merchant web site server forwarding the or a copy of the signed authentication/transaction token to the client agent (Step 356b). It is noted that in yet another embodiment, the transaction server may be placed in the same network as the business/merchant web server.

An in-house embodiment of the invention is illustrated in FIG. 3, an Internet

web server 110 configured as a transaction server 110 and having a coupled or associated database 113, such as an SQL/LDAP database, and storing user credentials in a database 115, and BWS 106 are coupled to each other and to other components of the system via a network, such as an intranet or extranet 129. End user devices 102, such as mobile phones, PDA's, notebook computers, or various hand-held devices also connect to the Internet/extranet 129 for access. Particularly when BWS 106 and transaction server 110 are connected over an extranet 129, other end users at remote locations may couple to the BWS 106 and TS 106 via the Internet 104. In this model, transaction server 110 is the in-house product. In this embodiment, the Internet 104 is used only to permit some end user 101 remote access to IWS or TS and BWS 106 on the intranet. Other than the nature of network connectivity, elements of the inventive system and method are as described herein above.

With reference to FIG. 4, structure and method provide for a second business and operating model and method which are primarily directed to a non-repudiation server as the authentication, electronic signature (e-signature) and non-repudiation Application Service Provider (ASP) on the Internet with a trusted partner. In this model, the interaction between the end user 101 through device 102, the non-repudiation server 110 with its LDAP database 113 and user Credential database 115 or their equivalent, and BWS 106 typically occurs over the Internet 104. The transaction non-repudiation server is operated as a service to validate a transaction or interaction between the end user device 102 and BWS 106. Note in the FIG. 4 embodiment, that details of BWS 106, transaction server 110, and mobile device 102 are as already described and not repeated here.

In another configuration, now described relative to FIG. 5, a Wireless Password Bank (WPB) is implemented using, for example, an EPOC (Symbian) based phone (such as for example but not limited to, a Nokia 9210 Communicator or Ericsson R380). A fingerprint sensor, scanner, or other capture add-on or build-in device with a respective Client Agent applet (for example a Java applet) and drivers is provided. A simple wireless server side Password Bank for WML Pages using, for example the X.509v3 private "bio" extensions (PBE) is also implemented.

The wireless password (PWD) bank embodiment may conveniently utilize a cellular or other mobile telephone handset as the end user device 102. It may also utilize any other communication device, wired or wireless, that includes the features utilized by the inventive technique. For example, the cellular handset or phone will include a biometric sensor 151 (such as a fingerprint sensor, microphone, and/or camera) with sensor data processing software, hardware, and/or other means, and a browser, such as microbrowser plug-in 171. The cellular phone communicates with a wireless receiver station 155, which in turn communicates to a wireless Internet gateway 156 via available wired or wireless communication means. Wireless Internet gateway 156 in turn couples through and inventive Wireless Password Filter 172 and from the Wireless Password Filter 172 via Internet 104 (or other means) to transaction server 110 as well as possibly to other Internet or world wide web-based sites or locations 173. For example, the system may be configured to communicate with such companies or portals as eticket.com, Schwab.com, eTrade.com, MyYahoo, or the like. Connectivity of such other sites 173 may be intermittent and dynamically changing. A direct wired or wireless communication link may also optionally be provided between the Wireless

Password Filter 172 and the transaction server 110. The transaction server 110 desirably includes a database (such as an LDAP database) storing user credential database, business data (such as XML documents), and transaction records. Typically, such database or databases are implied. Transaction server 110 may desirably also include a Password bank within the user credentials database.

In this wireless Password Bank, the client side program or applet (such as for example, a Java applet executed by a microbrowser) is or includes a simple plug-in or Java applet for the Microbrowser of a cell or other wireless phone or radio that controls the client side of the biometric authentication process. The wireless Password Filter also includes a plug-in (or other application) into the Wireless Gateway that filters out username/password requests from content or other web sites and replaces them with biometric authentication. This replacement process is advantageous because users tend to accumulate a lot of passwords for different sites and or services. Having to remember all of them, or even to type them in, is inconvenient. Simply storing the passwords on the device without some form of protection (a meta-password) would be a security risk. Therefore, releasing the stored passwords must be protected somehow, and in embodiments of the present invention passwords are protected with a biometric match of some sort (for example, using fingerprint biometrics). Note that in this embodiment, the passwords are stored on the transaction server 110, but they could also be stored on the client device 102 itself, which provides strong protection if secure storage exists that can only be unlocked by a biometric (such as for example, a smartcard or other securable memory device). After successful biometric authentication the filter 172 retrieves the username/password for the requested web site from the transaction server

110 and returns it to the web site server. The transaction server 110 provides the biometric authentication service for the wireless Password Filter as well as a server side password wallet where the various user name/password couplets are stored.

An exemplary embodiment of the transaction flow procedure 160 for the Wireless BioPDA™ embodiment is now described relative to FIG. 6. First, a user 101 indicates a desire to access a particular password-protected web site or portal, such as myyahoo.com (step 201) by directing the microbrowser to that particular web site or portal universal reference locator (URL). This request is directed to the myyahoo.com target site 173 from the microbrowser on the access device 102, through a wireless receiver station 155, wireless Internet gateway 156, and wireless password filter 172. Upon receipt of the request for access, the target site (such as for example, "myyahoo.com") 173, requests (step 202) username 193 and password 194 (or other sufficient identification) from the device 102 microbrowser. This request transits wireless password filter 172 and results in the initiation of execution (step 203) of the client agent applet 154. Execution of applet 154 results in the applet collecting and authenticating biometric information from the user 101 of the device 102 in conjunction with the transaction server. Once that biometric authentication has occurred, the transaction server, typically via an SSL or otherwise encrypted link, sends the username and password couplet information to the client agent 154. The client agent then supplies this information to the client microbrowser, and the client microbrowser in turn supplies this data to the originating website 106, 173 as if the user 101 had actually typed in the data them self. Execution of the applet 154 ultimately results in biometric capture (such as a fingerprint scan) which is used for a local biometric match (step

BNSDOCID: <WO 03007538A1_I_>

203B).

Once a local biometric match has been accomplished, the challenge/response authentication procedure (step 204) is performed between the client agent applet 154 executing on the client device 102 and the transaction server 110. This challenge/response authentication procedure may result in either a positive (confirmation of identity) authentication result or a negative (denial of identity) authentication result. When the challenge/response authentication procedure results in a positive authentication result, the transaction server sends a signed authentication/transaction token 157, in one embodiment in the form of a stored username and password information, to the client device (step 205). The client device and applet then decrypts it, sends the username/password to the client microbrowser, which in turn forwards it back through wireless Internet gateway 156 and back to the website that requested the information in the first place (step 206). No token need be sent back to the originating website.

Certain technical problems are overcome in the above described Wireless PWD Bank embodiment. For example, with respect to the client microbrowser, one embodiment provides or includes a client agent applet for an EPOC (Symbian) based browser that can communicate with the wireless password filter. An EPOC based browser is a browser that runs in a wireless phone and supports Java. The use of EPOC is advantageous at the present time as it supports Java and provides a documented SDK and architecture. Any of a built-in or external microphone, digital camera, or other biometric sensor or capture device, such as a fingerprint or other bioscanner may be added to device 102, such as for example by using a Multi-Media Card slot (Nokia 9210

phone), PC card slot, compact flash card slot, or other custom configuration. Wireless password filter is provided to filter and identify incoming HTML (or other identified format) username/password requests. A proxy, such as an HTML proxy server, may alternatively be implemented to provide this functionality. Also, in one embodiment the transaction server 110 includes a server component that provides the bioauthentication service as well as a user credential database and transaction logging within an LDAP compliant or other database. However, other browsers or user interfaces may readily be used instead. With respect to phone or handset hardware and operating system (or equivalent control), drivers are provided for EPOC that talk to the bioscanner or other biometric capture device and are accessible from the browser application.

Embodiments of the inventive system and method provide numerous advantageous features; including certain hardware, architectural, system, and server-side, client-side, and system software/firmware.

With respect to hardware features, for example, aspects of the invention provides a user device 102 having a rugged and low-cost (projected cost at about $5 or less per unit) silicon swipe fingerprint sensor suitable for mobile phone handset integration and the handset having such integrated (or add on or modular) sensor. In another aspect, the invention provides a rugged low cost printed circuit board (PCB) based finger print sensor that may readily be integrated into a mobile telephone, PDA, or other hand-held and/or portable wireless information appliance or device 102. Alternative embodiments provide support other than printed circuit board implementations, such as for example, a silicon substrate based swipe sensor.

While the above described biometric sensor hardware implementation has

considerable utility and provides advantageous features and capabilities, it will be appreciated that embodiments of the inventive system, method, and computer program and computer program product are not dependent upon any particular device 102 or biometric capture device or hardware within or attached to the device 102. The invention may be used with any off-the-shelf biometric sensor, such as those provided by Authentec, Identix, and Infineon, as well as others.

Where the biometric capture device is a fingerprint sensor, one embodiment of a finger print sensor is implemented as a silicon sensor involving a capacitive silicon swipe sensor technology. . This type of sensor provides the technological basis for high reliability as well as low-current and low-power consumption of it and its associated electronics. One embodiment generates a two-dimensional (2D) fingerprint image (or features extracted from the equivalent image) from a one-dimensional sensor. Using a one-dimensional sensor therefore permits the sensor to occupy a very small footprint, an advantageous feature given the small size of mobile phones and PDAs on which such sensor may be placed.

In one embodiment, the PCB based sensor is rugged and is integrated with the host device (e.g. mobile phone or PDA) very simply, as the PCB can be molded to conform to a desired shape. Inventive sensor electronics and sensor segment topology are a further aspect of the invention. Aspects of fingerprint (or other biometric) capture, reconstruction, matching and/or other software and/or firmware related processing are described herein elsewhere.

In another aspect, the invention provides client-side software/firmware having advantageous characteristics for a portable thin client device such as a mobile phone or

PDA. These characteristics include high-performance small footprint (small size) fingerprint extraction, matching, or other processing algorithms that may be stored within memory size constraints (size and cost) of cellular phones and execute within a processor of the device without undue processor requirements or burden on other processor loading. In at least one embodiment, the invention provides for fingerprint (or other biometric) matching on Subscriber Information Module (SIM), a technique referred to here as "Match-On-SIM." In another aspect, the invention provides a novel transaction non-repudiation applet as described above.

On the server and system side, embodiments of the invention provide non-repudiation server software and/or firmware. In another aspect, the invention implements biocertification methods and procedures. In a further aspect, the invention provides transaction non-repudiation software/firmware on the server side.

In conjunction with the use of a one-dimensional fingerprint sensor, a procedure which is conveniently implemented as a computer program executing in the processor and associated memory of the host device 102 is used to either construct a two-dimensional finger print from the (in effect a plurality of sequential) one-dimensional scans, or to extract the fingerprint features, commonly referred to as minutia, from the plurality of one dimensional scans without actually constructing the two-dimensional scan first. This later approach saves memory, and embodiments of the invention also save computations associated with reconstruction of the two-dimensional image and later recognizing the features, only to discard the raw two-dimensional scan. These techniques are referred to as the fingerprint or image reconstruction algorithm.

In another aspect, the invention provides fingerprint matching on the mobile device 102. Small, compact, or thin algorithms having sufficiently small amount of computer code and algorithms adapted for execution within the modest processor and memory capabilities (and cost) of typical mobile devices, particular cellular phone handsets. Recall that many non-repudiation transaction will involve financial transactions, such as purchases of goods or services, and financial investments such as the trading of stocks or bonds. Such transactions are made by mobile professionals and are most easily made using multi-purpose cellular telephones at a first level, and using PDAs and other mobile computing devices at a somewhat higher level.

In one embodiment, the fingerprint matching algorithm software resides in less than 50 Kbytes of ROM or RAM and has low computational requirements. In one embodiment, the fingerprint matching algorithm is operative to perform a Match-on-SIM. Match on SIM refers to having the biometric matching algorithm running on the CPU of the SIM card itself. This allows the SIM card to be used as a secure storage mechanism. SIMs have a small CPU and some user read/writable memory. This memory is typically unlocked (made available to the SIM's host hardware, such as the cell phone) through the use of a Person Identification Number (PIN) typed in the by user. In a Match-on-SIM card, instead of typing the PIN, the user can use his/her biometric data instead. The client agent applet would prompt the user to, for instance, place his/her finger on the fingerprint sensor. The biometric data would then be sent into the SIM to be authenticated. If the SIM indeed authenticates the user's biometric data, then the SIM can unlock its secure memory area and allow it to be read from and written to by the cell phone's application software. This eliminates the inconvenience of user's

typing in a PIN, and in addition, provides secure storage for user credentials (as in the password bank described above) or private keys or any other secrets.

In another aspect, the Non-Repudiation Applet embodies an elegant solution to client and user authentication that desirably use a Java security memory model, is downloadable and ungradable, portable, and easily integrated into a merchant's or other's web pages. An open application program interface (open API) is desirably provided so that third-party biometrics providers can plug-n-play.

In still another aspect, the invention provides voice or speech recognition and matching. This is optionally but desirably provided on a SIM within the device to provide a Voice Match-on-SIM in addition to or instead of the Fingerprint Match-on-SIM. Hashing algorithms are desirably utilized to enable database privacy and security for any biometric data.

Further aspects of some of the optional technology that may beneficially be applied to the inventive system and method are now described. Biocertificates are one particularly significant aspect of certain embodiments of the invention, though not of other aspects. In one embodiment, the Biocertificates are based at least in part on the standard Internet X.509 Version 3 (X.509v3) Public Key Infrastructure Certificates and related protocol promulgated in 1996. Internet X.509 PKI generally is an evolving standard known in the art. References to this standard refer to the versions existent in June 2001, for example CCITT Recommendation X.509 (1988), "The Directory - Authentication Framework" as well as IETF RFC 1422. The Biocertificates may be embedded as private extensions or attached as attribute certificates to the standard X.509 ID certificates. The private extensions and/or attribute certificates may similarly

be applied to other standard or non-standard certificates other than X.509 certificates and such X.509 certificates are described only by way of example not by way of limitation.

In one embodiment described with reference to FIG. 7, it is assumed that the X.509 based certificate 240 includes several fields or components however organized, including: Version 241, Certificate Serial Number 242, Signature Algorithm Identifier 243, Issuer Name 244, Validity Period 245, Subject Name 246, Subject Public Key Information 247, Issuer Unique Identifier 248, and Subject Unique Identifier 249. An extensions filed or component is also permitted within the X.509 certificate and may normally be empty or contain other than the inventive bioextensions. These standard fields are known in the art, available from the published standards, and not described in further detail here.

When the Biocertificate is embedded as a private extension in the extensions field 250, one embodiment of the private extension provides the following fields or components: Enrollment Trust Level 251, Protection Trust Level 252, Common Bio Header Field 253, and an encryption {Encr. (Key_{Pub} ICTS) [Template]} 254, "Template" 254c is the extracted biometric information such as the fingerprint minutia used for fingerprint comparison and matching.

Private Bio Extensions (PBEs) have certain advantages and disadvantages. Advantageously, they provide all necessary information in one certificate; since the extensions are non-critical to some applications, the PBE information can be ignored by those applications that do not need it or do not know about it; acceptance for X.509v3

private extensions is well established; and standard Certificate Authorities and Revocation Lists and structures can be used.

Disadvantageously, all information in the X.509 certificate is meant to be public, and it follows that any attribute placed in an X.509 certificate cannot be kept confidential unless other measures are taken. Furthermore, the information in the certificate is tied to the life span of the certificate itself. Finally, the Biometric information has to be available during registration, and existing certificates can be problematic for certain of the applications.

Rather than PBEs, BioAttribute Certificates (BAC) 258 includes an ID certificate 259 and an attribute certificate 260 and may alternatively be used and are now described relative to FIG. 8. In one embodiment, the BioAttribute certificate 260 is an X.509-based Attribute certificate. One exemplary embodiment links the ID Certificate 259 Serial Number 262 of the X.509 ID certificate with the Holder 272 of the Attribute certificate 260. The Attribute certificate 260 includes fields or components for Version 271, Holder 272, Certificate Issuer 273, Algorithm Identifier 274, Certificate Serial Number 275, Validity Period 276, Enrollment Trust Level 277, Protection Trust Level 278, Common Bio Header Field 279, and Encr. (Key_{Pub} ICTS) [Template] 280.

As with the use of PBEs 240, the use of BACs 258 has advantages and disadvantages. For example, advantageously, the BACs 258 works with existing certificates so that no re-issue certificate is necessary. The content can be encrypted. The attribute certificate can be signed by the ICTS server. Applications that are not aware or don't want to use BAC 258 can use the original X.509 (for example, to

increase speed). The Lifetime of the attribute certificate can be different than base certificate.

Disadvantageously for the use of BACs, two signatures have to be created, the X.509 ID certificate 259 and the X.509 Attribute certificate 260. In order to perform the bioauthentication signatures have to be verified which increases complexity and processing time. Finally, attribute certificate are usually used for short-lifetime information, such as for example, for authorization information.

While X.509 based certificates are described by way of example of the types of certificate or certificate information that may be used, it will be understood that other forms of biometric containing certificate may be used. Any file, data structure, date, code or other instrument containing a wrapped biometric, that is a combination of biometric data and a public key that is part of a public/private key pair used for encryption, decryption and cryptographic signing, may be used.

An embodiment of a transaction token 320 is now described relative to FIG. 9. Upon successful authentication and/or signing of the transaction, the transaction server system generates a unique transaction token 320 that is passed back to the Server Agent 107 on the Business Web Server 106. The Business Web Server 106 stores this token 320 within it's own transaction log. In addition, the transaction token 320 can be used to access (request) the document or other content, such as an XML document, for that particular Business Web Server 106 and user 101 that the system maintains. An exemplary embodiment of the format and content of a Transaction Token 320 is now described.

The exemplary transaction token 320 includes a globally unique Transaction ID

332 that is used to reference a transaction on all of the involved sides (servers and with client). In one embodiment, the Transaction ID 322 includes: (a) a time or time stamp 323, where the time is advantageously an absolute time such as GMT (rather than a local time) and of high resolution; (b) a task or process identifier (PID) 324; (c) a machine or server identifier (Server Name) 325; and (d) a user identifier (User ID) 326. In one embodiment, transaction ID do not expire, such as when a communication connection is dropped or lost, so that audit requirements may be maintained.

In one embodiment, a logging and auditing mechanism and record takes place on the transaction server 110, including a transaction log recording what happened with a created transaction token 320. This transaction token 320 is, in one embodiment, a subset of transaction record 310. The transaction record 310 includes: (i) a Transaction ID 322 in the transaction token 320, (ii) Business Web Server name 327, (iii) ICTS or transaction server name 328, (iv) Transaction Data 329 (optional depending on Business Web Server Policy: clear text, hash, encrypted with Business Web Server public key or void), (v) Time Stamp (e.g. GMT) 323 within transaction token 320, (vi) Security policy required by Business Web Server 330, (vii) Security policy used 331, (viii) Common biometric header format (CBEFF) 332, (ix) Used biometric template 333, (x) User ID (ICTS or transaction server user ID) 334, (xi) Certificate Serial number 335, (xii) Attribute Cert Serial number 336, (xiii) Signature format (used hash or the like) 337, (xiv) Hash of transaction data 338, (xv) Signed hash of the above 339. It will be appreciated that not all of these items or fields in the record are required in all embodiments and that some are optionally but advantageously provided.

The data contained in the Transaction Token 320 can be configured as a policy setting per Business Web Server 106 and may be different for different policies and/or for different Business Web Servers, and is equal to, or a subset of, the data stored in the transaction record 310. While not representing a minimum configuration, the following default setting and contents or items may be used: Transaction ID 322, Security policy required by Business Web Server 330, Security policy used 331, User ID (ICTS or transaction server user ID) 334, Time Stamp 323, Hash of Transaction Data 338, Signature format 337, and Signed hash of the above 339.

An Authentication Token is used to confirm a successful transaction authentication. One embodiment of the authentication token includes the following fields or elements: Transaction ID, Security policy required by Business Web Server, Security policy used, User ID (ICTS or transaction server user ID), Time Stamp, Requested resource (URL), Signature format, and Signed hash of the above. Note that the authentication token may be considered to be a special type of transaction token 320, it has the URL requested as the "transaction data" 329, and the signature is the signature of the "transaction server" performing the authentication.

An embodiment of the user enrollment process 410 is now described. In the exemplary embodiment now described, user 101 initiates the enrollment process via a dedicated page or "registration" button on the Business Web Server 106 where the Business Web Server may either adopt some default enrollment requirements or can define specific enrollment requirements. For example, specifying the type of biometric (finger print, face recognition, retinal scan, voice print, or other biometrics known in the

art), number of samples, type of enrollment (face-to-face, over-the-air self-enrollment, or the like) (Step 411).

A trusted Client Agent program, such as an applet or ActiveX control, on the client device (such as a Compaq iPaq, Palm Pilot, Handspring, Sony Clie PDA or other intelligent device) – is initiated and its enrollment function is started, where trust may be established using standard code signing technologies (Step 412).

A SSL/TLS session between the client device browser and the ICTS or transaction server Biometric Registration Authority (BioRA) is established by using the ICTS/BioRA server's X.509 certificate (Step 413). The Client Agent requests the user's username and any additional information necessary for the generation of a certificate, such as the X.509 based Certificate (Step 414). An email address for example may be one of the required additional information items. Upon receipt of the request, the user fills out necessary information and submits the information; and the client device optionally performs local plausibility checks on the information, such as whether all required fields have been provided or where only numbers have been submitted where a number entry is required (Step 415).

The Client Agent on the PDA generates the user's RSA key pair (for transaction non-repudiation purposes), compiles the necessary user information and sends the X.509 Certificate request (using for example a PKCS #10) to the BioRA (Step 416).

A user's private key will be stored in local key store encrypted with a user specific password, and in a separate local table (local user table) a new entry will be added with the userID and an MD 5 or SHA-1 hash of the users password (Step 417).

BNSDOCID: <WO 03007538A1 | >

After appropriate request handling on the BioRA, the BioRA forwards the X.509 certificate request to external PKI CA, using for example PKCS #10 (Step 418).

An entry is logged at the BioRA indicating the successful transmission or forwarding of the X.509 certificate request for user XXX (where XXX refers to a user identification) to certificate authority ZZZ (where ZZZ refers to a certificate authority identification) at the identified date and time (Step 419). The signed X.509 certificate is received from the (external) PKI certificate authority (Step 420). An entry is logged at BioRA indicating the successful receipt of the X.509 certificate for user XXX from certificate authority at ZZZ date and time (Step 421).

The BioRA forwards the signed X.509 certificate to the client device and generates a log entry indicated that it forwarded the X.509 certificate to user XXX at date and time (Step 422).

Through the Client Agent, the BioRA acquires the initial biometric template(s) in accordance with the enrollment policy (Step 423). The Client Agent's enrollment function then collects any necessary additional user data (that is not part of the standard X.509 certificate, such as for example a credit card number or other information) and together with the biometric template creates the system specific Attribute Certificate, such as an Attribute Certificate XML structure. In addition the user's biometric templates are stored unencrypted in the local user table (Step 424).

On the client device, the user's biometric template or templates are then encrypted using the user's RSA public key (Step 425), for example according to the W3C "XML Encryption Requirements, W3C Working Draft, version of 2001-April-20, incorporated herein by reference

On the client device, the Attribute Certificate XML structure (See Step 424) is then digitally signed with the user's private key (See Step 416) following the IETF "XML-Signature Syntax and Processing", draft-ietf-xmldsig-core-08.txt, [XMLDigSig] procedures as a proof-of-possession of the PKI private key associated with the certificate, received from the PKI CA (Step 426).

The Client Agent submits the request (including the XML structure) for the inventive IControl BioAttribute Certificate to the BioRA, and a log entry for this request is generated on user's client device (Step 427).

The BioRA on the ICTS or transaction server verifies the signature on the received signed BioAttribute Certificate XML document by using the users X.509 certificate (Step 428). Next, the BioRA on the ICTS transaction server uses the ICTS RSA signing key to sign (or counter-sign) the users XML document including the encrypted biometric template, the additional user data (such as the enrollment attributes) as well as the user's signature of the XML document using for example the [XMLDigSig] to generate the user's system IControl BioAttribute Certificate (Step 429). The IControl BioAttribute Certificate is stored in a ICTS directory and then sent back to the user's device for subsequent use in transaction signing processes (Step 430).

On the BioRA of the ICTS, the completion of the generation of the user's IControl BioAttribute Certificate is logged (Step 431), and on the client device or PDA, the user is provided with feedback (such as a message) regarding the successful generation of his BioAttribute Certificate, and a respective local log entry is created (Step 432).

An exemplary embodiment of the Transaction Signing process, which in some embodiments includes the client-side biometric match, is now described. Transaction signing using Public-Key Infrastructure (PKI) requires the establishment of the signer's public key credential, the PKI certificate. The introduction of biometrics to the process is largely for enhancing the identification of the signer, before the signer utilizes their PKI private key to digitally sign a transaction. An additional value in the use of biometrics is that of providing a secure, convenient-user experience.

The typical PKI user must input a Personal Identification Number (PIN) to the computing station, user device, or information appliance that contains the signer's PKI private key before the signer can use the private key to apply their digital signature. In many cases this PIN is used as an encryption agent in protecting the signer's PKI private key. It is conceivable that a PKI private key protection agent on the signer's computing station could acquire the user biometric information (BioID), evaluate this BioID against a BioID enrollment template, and allow use of the protected PKI private key to generate a digital signature or establish a secure communications channel.

A security difficulty lies in the full-time protection of the PKI private key in a generally, unsecured computing environment. The quality of a security process to protect this key is often measured by three factors: (i) something you have (such as the computing station or device that contains the PKI private key); (ii) something you know (such as a PIN that is used to cryptographically lock the PKI private key); and (iii) something or someone you are (such as the biometric information used to apply the above PIN to unlock the PKI private key).

While requiring the entry of a PIN each time the PKI private key is required for use is considered good security, it's being acquired for each use is not considered a secure, convenient user experience. This is especially true if the signer's computing station is not ergonomically designed for convenient entry of the PIN, such as may be the case for a typical cell phone or PDA. Enhancing the user's experience along with an understood acceptable level-of-risk encourages the relaxation on requiring the PIN for every PKI private key use. Therefore embodiment of the invention that require PIN entry for every PKI private key use and embodiments that do not so require PIN entry for every PKI private key use are contemplated by the invention.

From a convenience perspective not ever requiring the PIN is most appealing. Using the BioID value to "unlock" the PKI private key would provide an agreeable level-of-risk. This is particularly appealing if the PKI private key is generally protected from prying eyes on the signer's computing station. Specialized computing stations, such as smart cards or subscriber identity module (SIM), do not allow any external access to the PKI private key. Such is not the case in a general-purpose computing station.

Software cryptographic protection of the PKI private key is used to minimize the window of opportunity to externally acquire the PKI private key. If the BioID were deterministic rather than probabilistic in value, then the BioID could be used as the cryptographic key to lock access to the PKI private key. Such is not the case. Either the PKI private key will need to be embedded in the BioID evaluation software with the acceptable level-of-risk being the unlikelihood that the compiled evaluation software

will be acquired and decoded for unacceptable use; or, the PKI private key must be cryptographically encoded by other means with an acceptable level-of-risk.

The structures and methods described herein, including the use of the transaction token, provide procedures having an acceptable level-of-risk for many transaction environments, and also possessing appealing user-convenience characteristics.

It is noted that in some of the embodiments described herein, it is assumed that no secure storage such as a smart-card based SIM exists in the system, so that a password is needed to decrypt or unencrypt the stored secrets. If secure storage does exist, however, then all the secrets (such as passwords and/or private keys) can be stored using the secure storage and unlocked with a biometric match. Provision of the smart-card, SIM, or other protectable or secure storage, also permits the so called match-on-SIM or match-on-smart-card functionality.

Other Exemplary Aspects and Features

Aspects of the invention provide true transaction non-repudiation on a wireless device and ensure that both the sender and the receiver are who they say they are and facilitate creation and operation of an insurable wireless transaction.

At a top level, the inventive system, method, and computer program produce software enables confident, trusted, electronic and mobile commerce (mCommerce). Convenience is facilitated by permitting customers to create and log-in to personal accounts without cumbersome Personal identification numbers or codes (PINs) and passwords. This feature encourages increased usage and new subscribers. The invention also provides transaction non-repudiation so that service providers and

merchants capture proof-positive transaction audit trails that mitigate repudiation risk. Privacy is enhanced so that customers gain confidence in the confidentiality of their transactions, thereby encouraging increased usage and new subscribers. Security is provided at a level that customers gain trust in the security of their personal accounts and personal information, again encouraging increased usage and new subscribers.

The invention permits and supports authentication at any one or more of several levels using a variety of authentication options. These options include but are not limited to passwords, tokens, smart cards, digital certificates, and biometrics. Biometrics includes but is not limited to fingerprint or fingerprint derived biometrics, retinal imaged or scanned biometrics, voice or speech based biometrics, molecule based Biometrics, or other biometric or biometrically derived data.

The authentication options are or may be combined with any one or more of available devices, particularly mobile devices such as mobile or cell phones, PDA's, hybrid PDA and mobile phones, and personal computers (PCs) or other information appliances.

It is noted that the inventive system and method have numerous advantages over conventional systems and methods. These advantages may include one, more, or all in any particular embodiment, but are not limited to: (i) multiple levels of authentication from moderate (passwords) to strong (digital certificates) to very strong (biometrics); (ii) flexible, layered authentication alternatives; (iii) vendor independence for authentication methods and devices; (iv) client-side applet is device independent (for example Java-based client-side applet); (v) powerful, back-end authentication web server; (vi) highly scalable to millions of users; (vii) easily deployed and integrated to

existing Web applications; and (viii) can be deployed either as a licensed product and as a service.

From the standpoint of a business model and method, deployment and/or operation of aspects and embodiments of the invention may provide for deployment as a licensed product or as an out-sourced service. When deployed as a licensed product, customers may for example, license the client side products on a per user basis along with the server software. License produce may alternatively license the products on a per week, per month, annual, or on any other time-based, transaction-based, percentage of transaction amount based, or other basis.

When deployed as an out-sourced service, aspects and embodiments of the inventive system and method provide an authentication, e-signature and transaction non-repudiation service on the Internet or over any other public or private network.

The foregoing description, for purposes of explanation, used specific nomenclature to provide a thorough understanding of the invention. However, it will be apparent to one skilled in the art in light of the description provided that the specific details are not required in order to practice the invention. Thus, the foregoing descriptions of specific embodiments of the present invention are presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the invention to the precise forms disclosed, obviously many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications, to thereby enable others skilled in the art to best utilize the invention and

various embodiments with various modifications as are suited to the particular use contemplated.

We Claim:

1. A transaction authentication and non-repudiation system comprising:

a transaction server intermittently coupleable to other information processing devices over a network;

said transaction server including or coupleable to a database storing at least one user credential and at least one transaction record;

said transaction server including a processor and a memory coupled to said processor for executing transaction authentication instructions.

2. The system in claim 1, wherein said transaction authentication instructions include instructions for a challenge/response authentication.

3. The system in claim 2, wherein said transaction authentication instructions include instructions for sending a signed authentication/transaction token.

4. The system in claim 3, wherein said sent signed authentication/transaction token is sent to an external client agent computer program executing in processor and coupled memory in an external client device.

5. The system in claim 4, wherein said external client device comprises a wireless device.

6. The system in claim 3, wherein said transaction authentication instructions include instructions for communicating with a server agent computer program on an external business/merchant web server.

7. The system in claim 1, wherein said at least one user credential comprises a plurality of user credentials.

8. The system in claim 1, wherein said at least one transaction record comprises a plurality of transaction records.

9. The system in claim 1, wherein said at least one user credential comprises at least one of a biocertificate, a certificate chain, a merchant data, and combinations thereof.

10. The system in claim 1, wherein said transaction server includes or is coupleable to a biometric registration authority.

11. The system in claim 10, wherein said biometric registration authority comprises an X.509v3-based certificate authority.

12. The system in claim 10, wherein said biometric registration authority comprises an X.509v3 certificate revocation list.

13. The system in claim 10, wherein said network comprises a global network of interconnected computers and information appliances.

14. The system in claim 13, wherein said global network of interconnected computers and information appliances comprises the Internet.

15. The system in claim 1, wherein said other information processing devices include a client device.

16. The system in claim 1, wherein said other information processing devices include a business/merchant web server.

17. The system in claim 1, wherein said other information processing devices include a client device and a business/merchant web server.

18. The system in claim 17, wherein said client device includes wireless communication means for communicating with said network.

19. The system in claim 18, wherein said wireless communication means includes a radio-frequency communication modem for coupling to said network via a wireless network gateway.

20. The system in claim 19, wherein said wireless network gateway comprises a wireless Internet gateway.

21. The system in claim 18, wherein communications over said network are conducted using WML, HTML, WAP/HTML, CHTML, xHTML, and combinations, subsets, or extensions thereof.

22. The system in claim 17, wherein the client device includes a client agent for performing a local biometric matching.

23. The system in claim 22, wherein said client device further includes a biometric sampling component for obtaining a biometric sample from a user.

24. The system in claim 23, wherein said biometric sample comprises a biometric sample selected from the set consisting or a fingerprint sample, a face image sample, a retinal scan sample, a voice sample, a genetic sample, and combinations thereof.

25. The system in claim 17, wherein said business/merchant web server comprises a server agent.

26. The system in claim 25, wherein said server agent is implemented as a computer program including computer program instructions executing on a processor and memory of said business web server.

27. The system in claim 22, wherein said client agent is implemented as a computer program including computer program instructions executing on a processor and memory of said client device.

28. The system in claim 1, wherein said transaction server includes a computer program including computer program instructions executing on a processor and memory of said transaction server.

29. The system in claim 17, wherein said business/merchant web server includes or is coupleable to a banking infrastructure or entity.

30. The system in claim 17, wherein said business/merchant web server includes or is coupleable to a financial transaction infrastructure or entity.

31. The system in claim 17, wherein said business/merchant web server includes or is coupleable to a stock, security, or bond purchase or sale transaction infrastructure or entity.

32. The system in claim 21, wherein the communications over the network include communications built upon an underlying TCP/IP protocol.

33. The system in claim 32, wherein the communications include a WAP/HTLM over TCP/IP protocol or improvement or extension thereof.

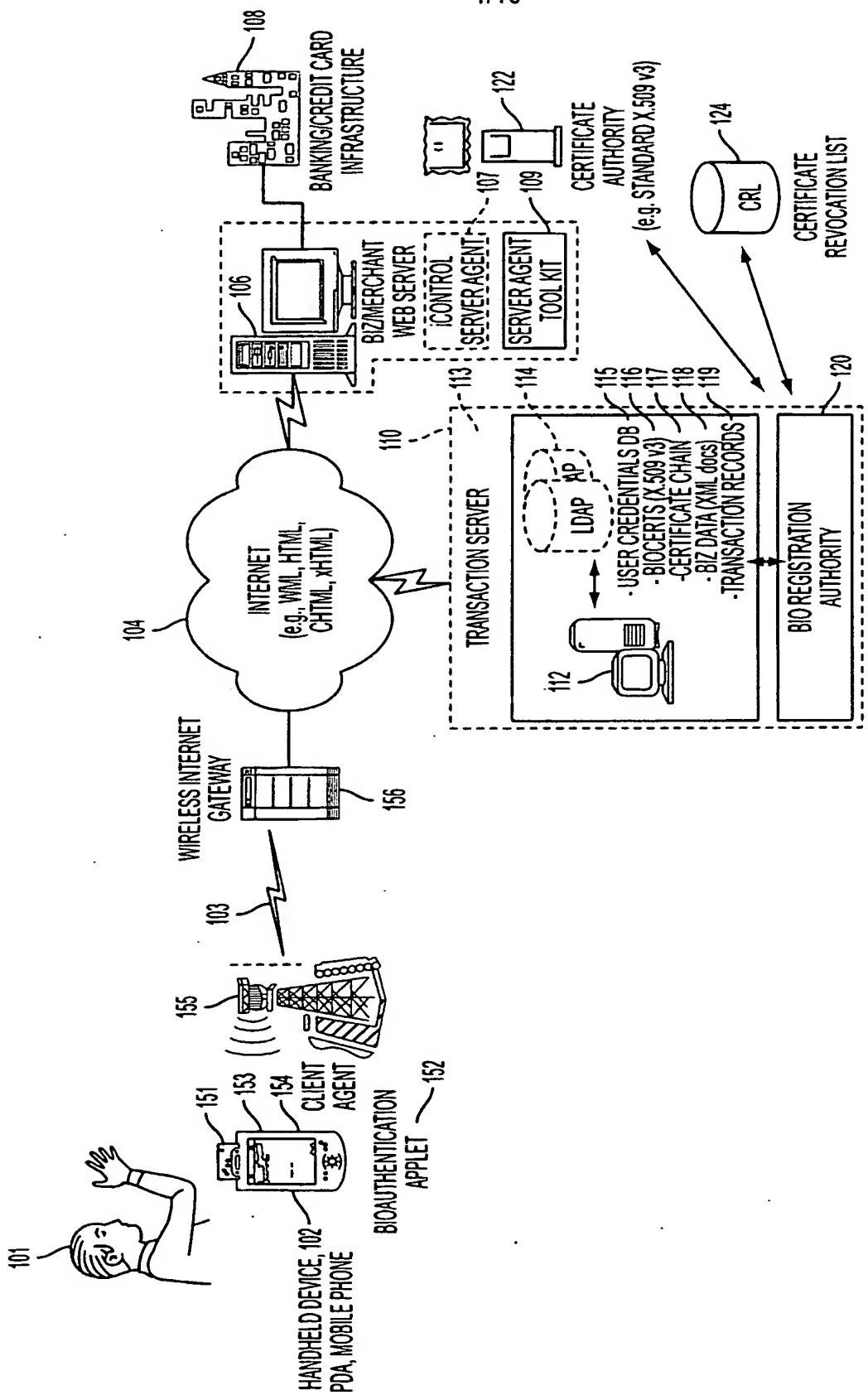


FIG. 1

BNSDOCID: <WO_____03007538A1_I_>

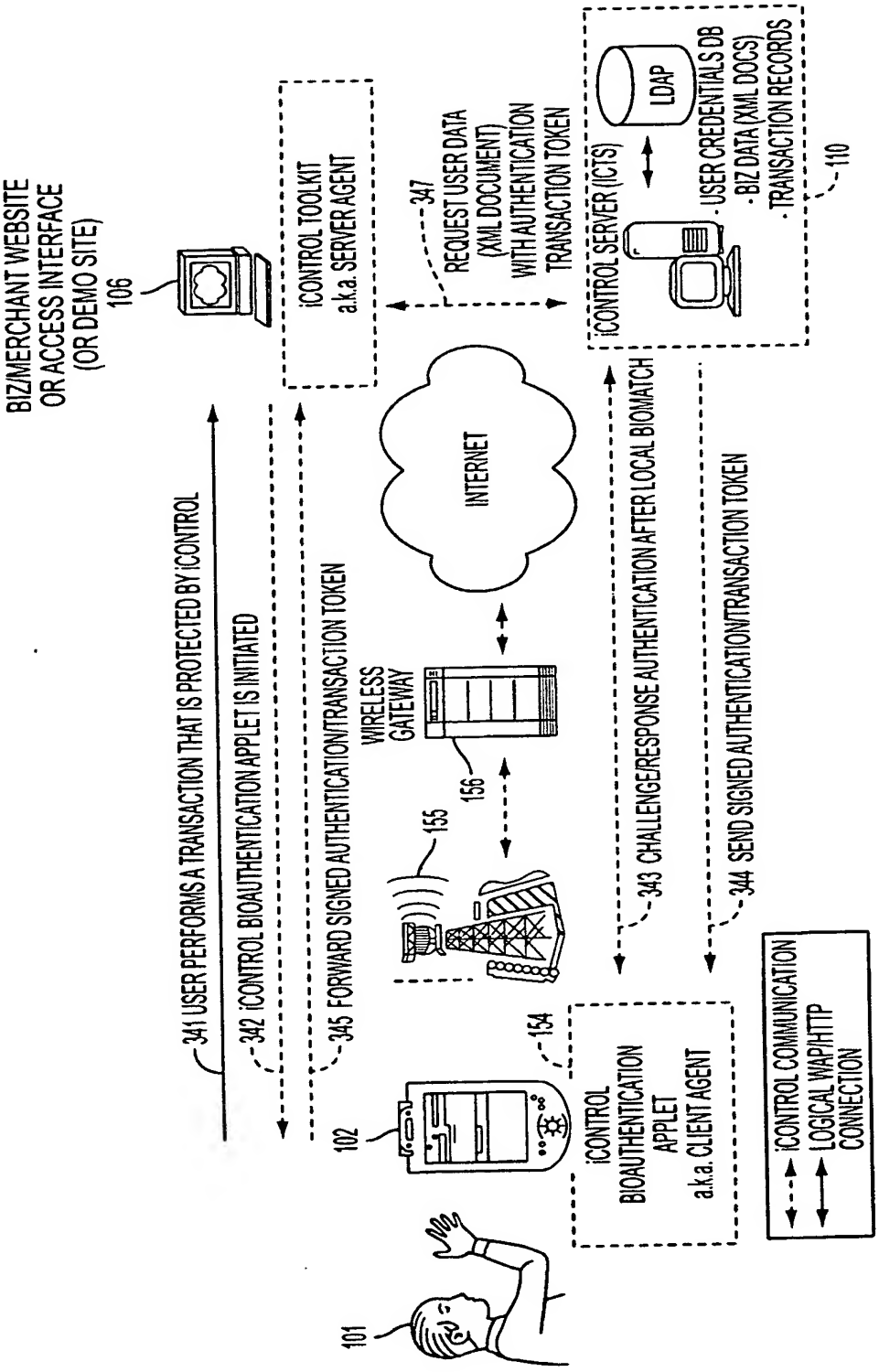


FIG. 2A

BNSDOCID: <WO 03007538A1_I_>

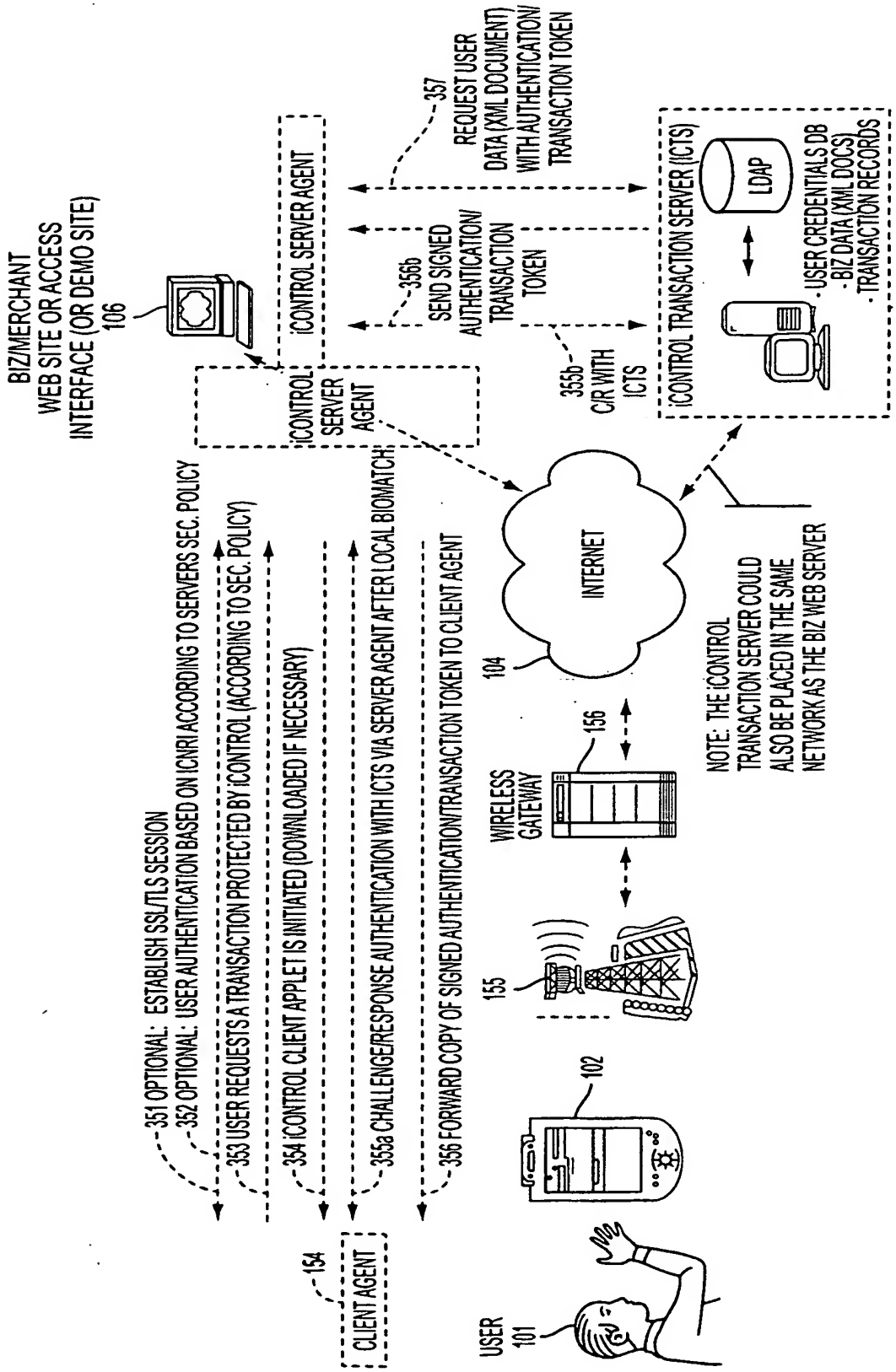


FIG. 2B

BNSDOCID: <WO_____03007538A1_I_>

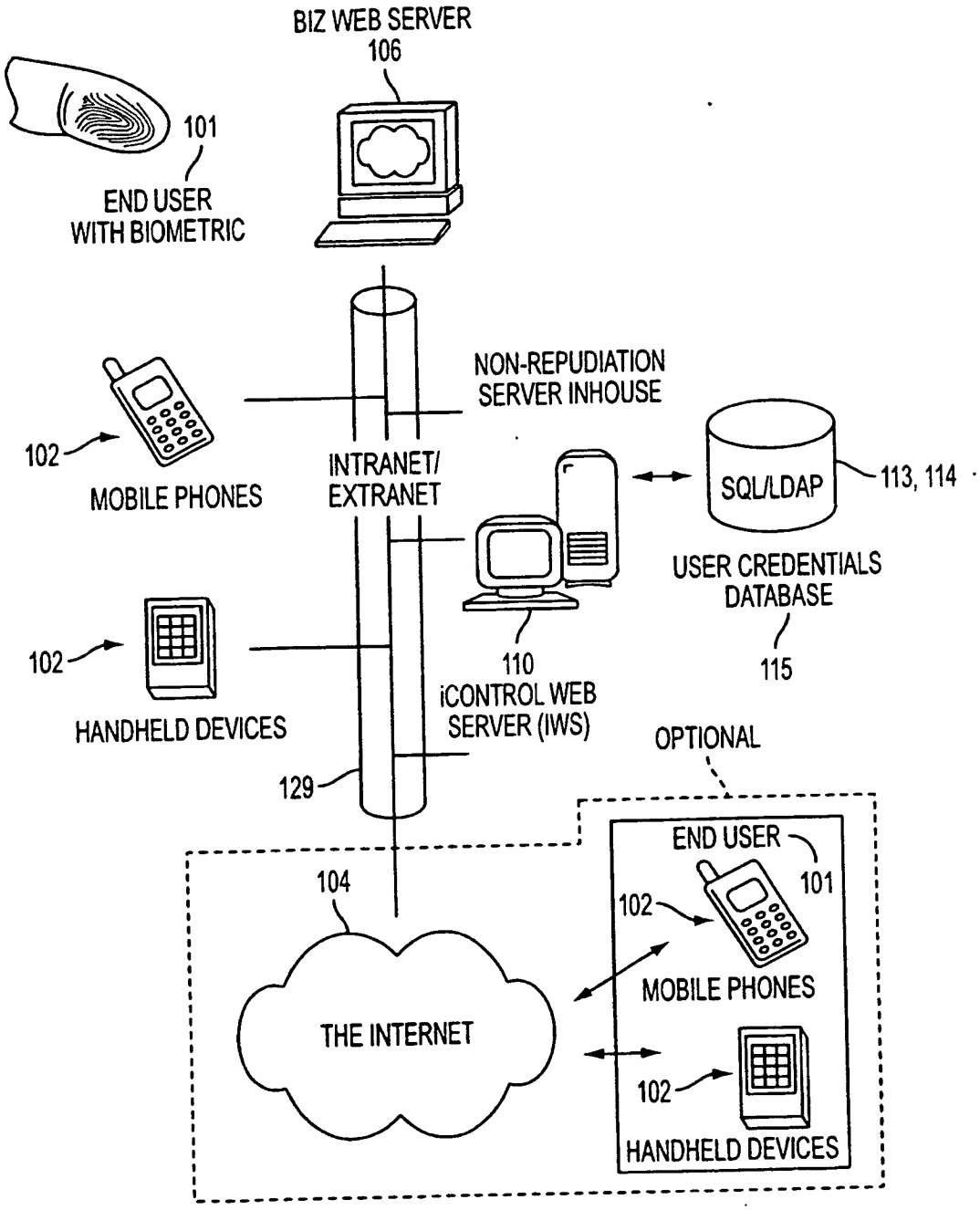


FIG. 3

BNSDOCID: <WO 03007538A1 | >

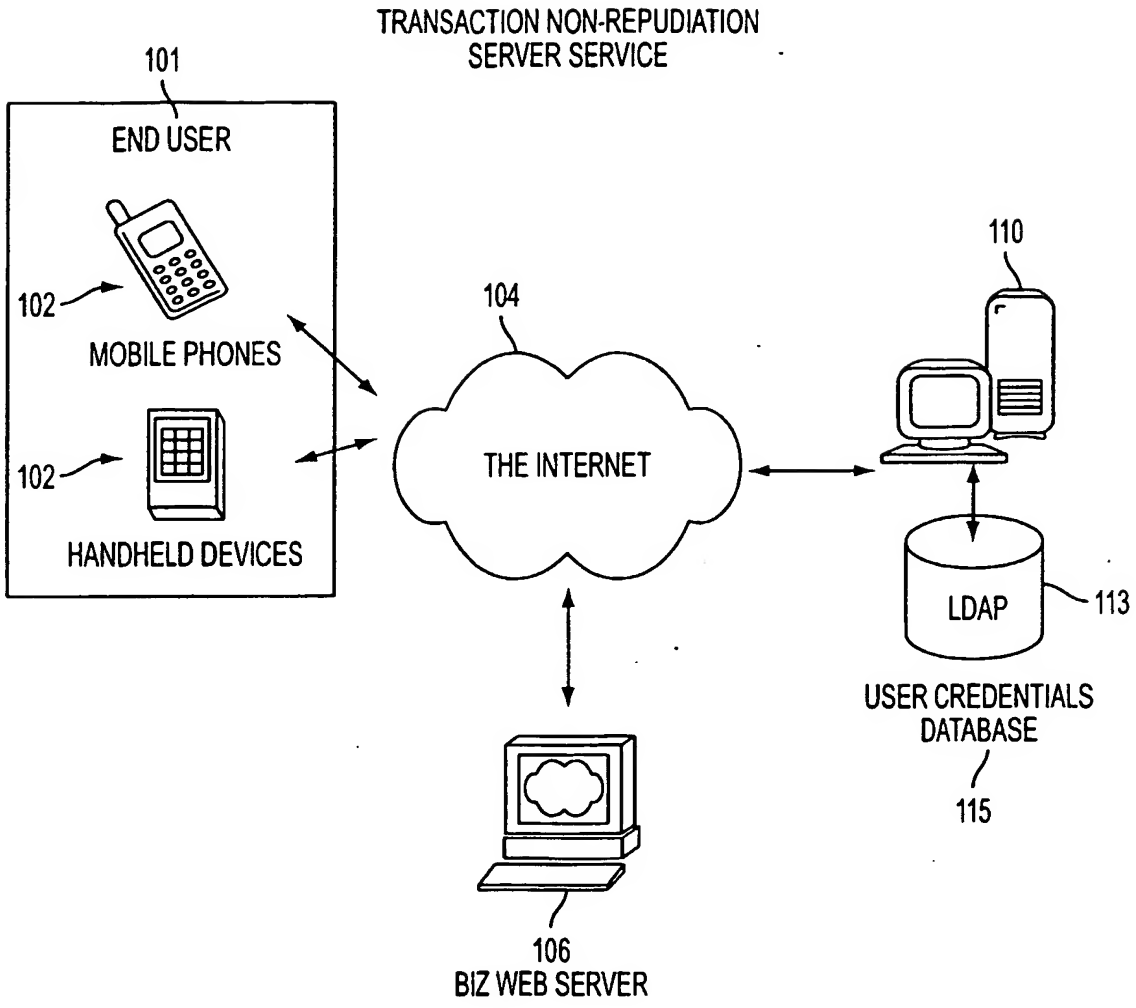


FIG. 4

BNSDOCID: <WO_____03007538A1_I_>

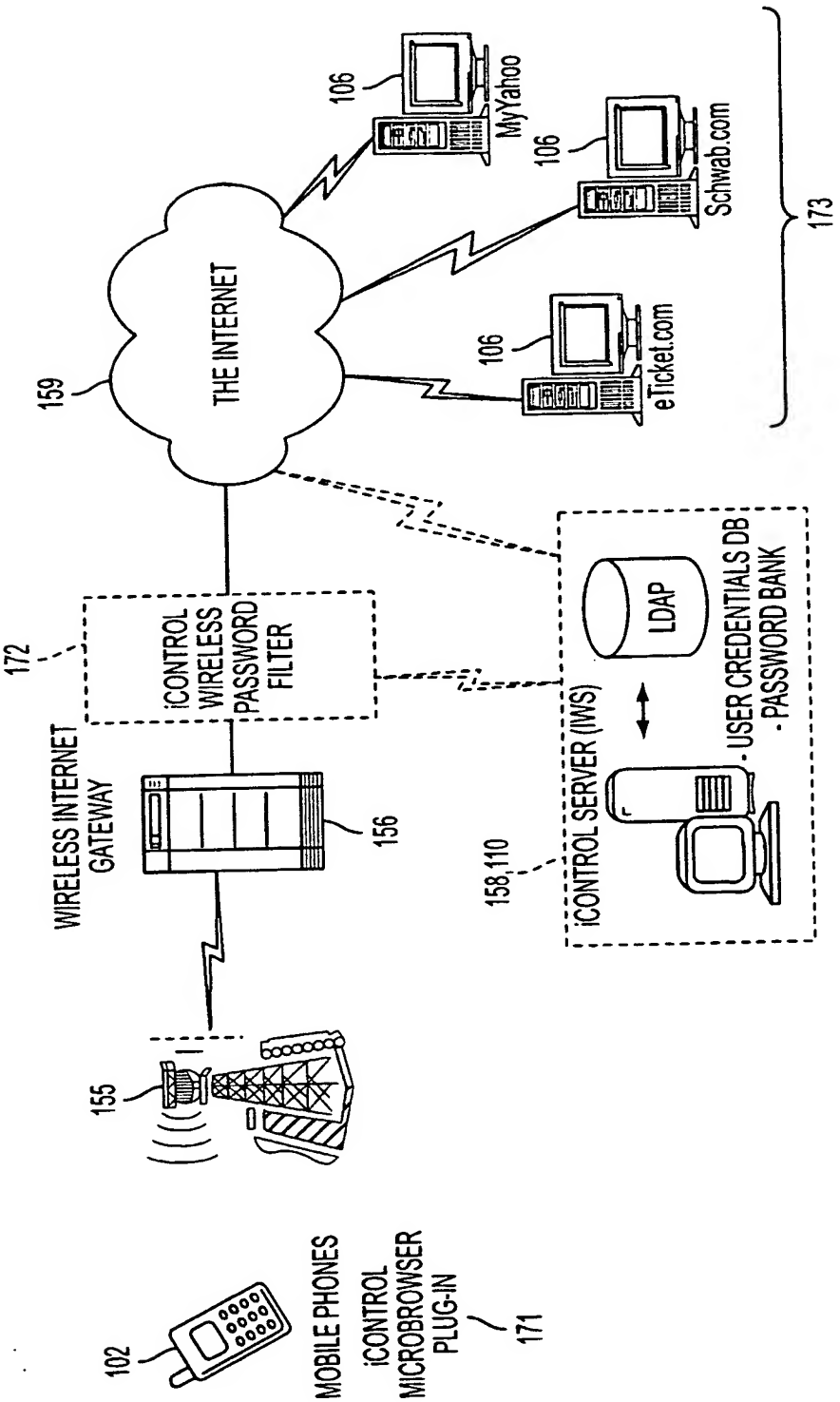


FIG. 5

BNSDOCID: <WO 03007538A1 | >

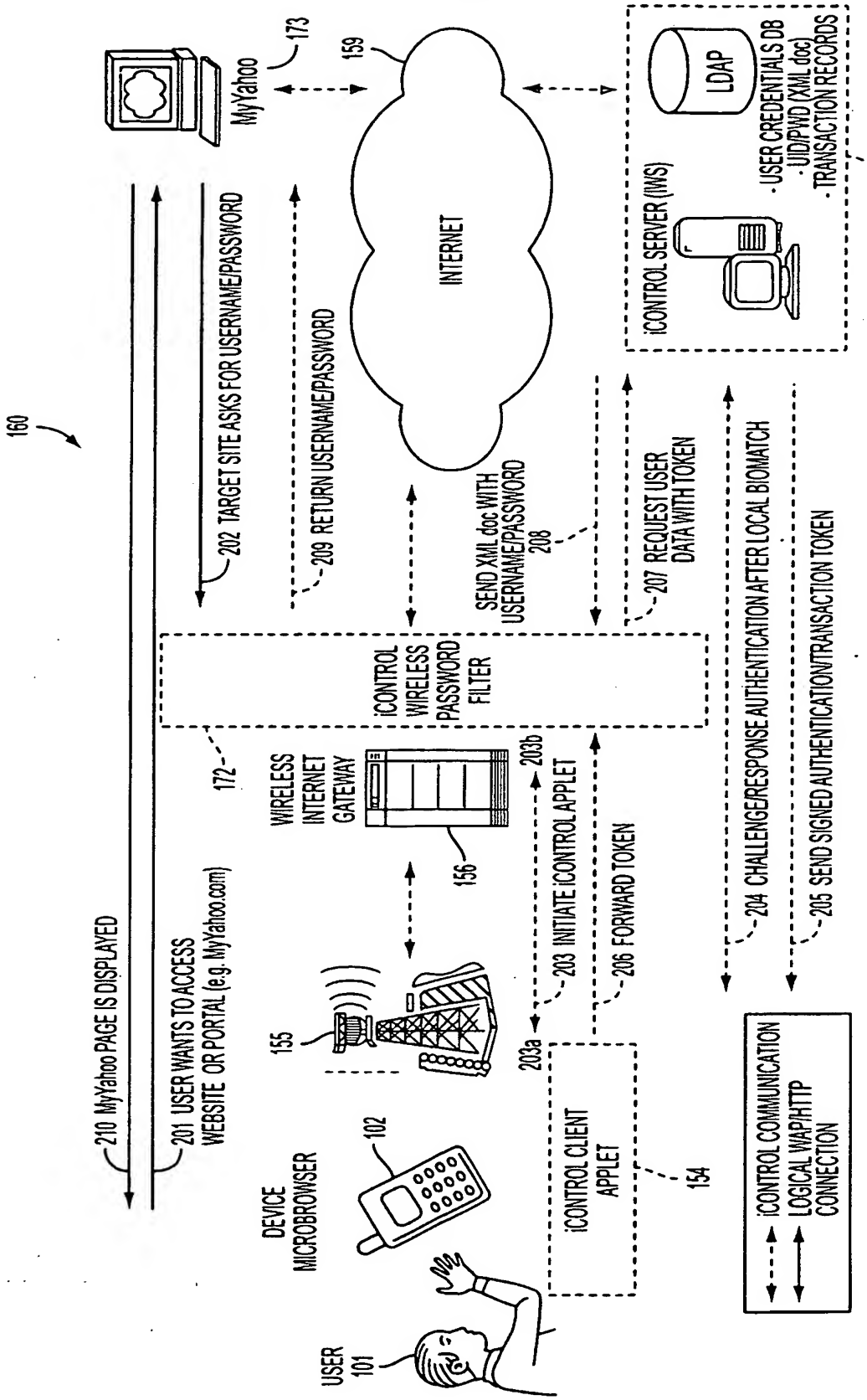


FIG. 6

BNSDOCID: <WO_____03007538A1_I_>

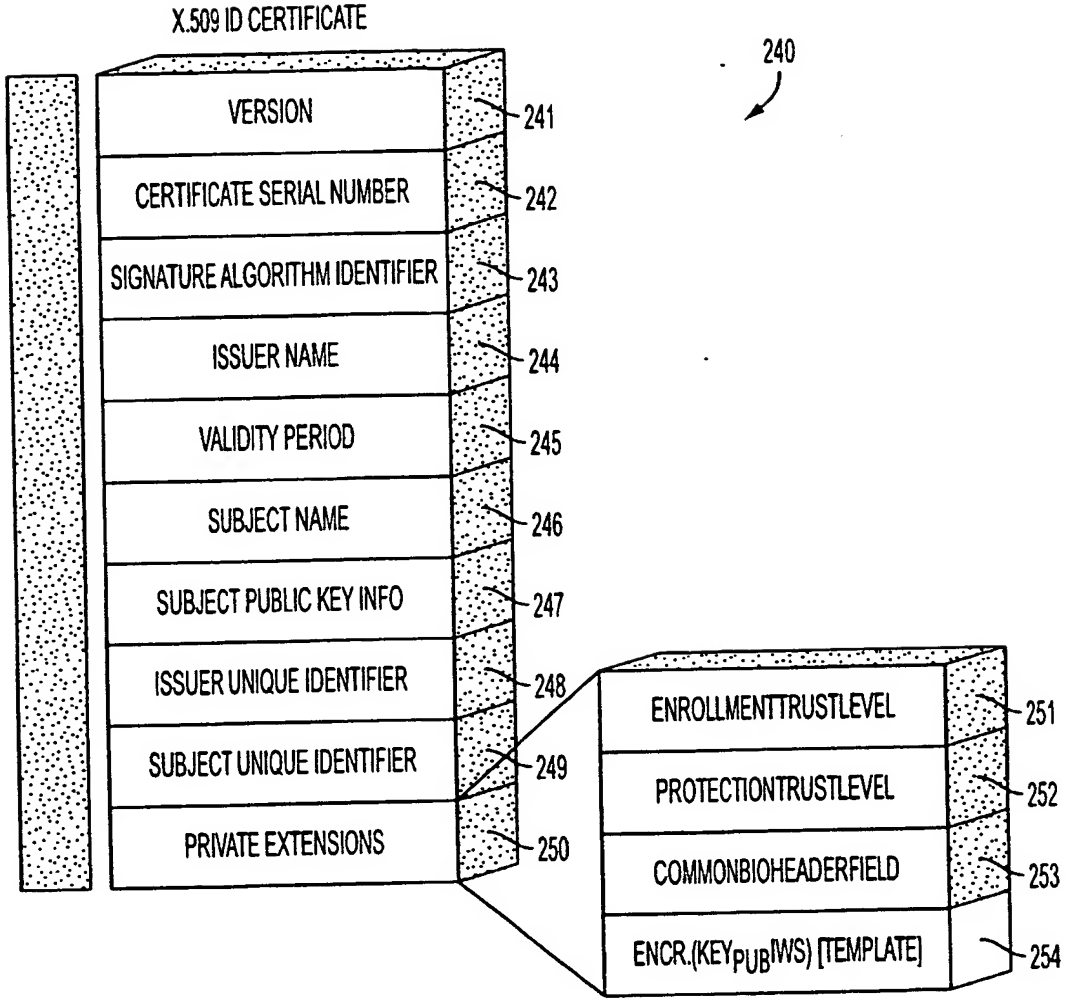


FIG. 7

BNSDOCID: <WO 03007538A1 | >

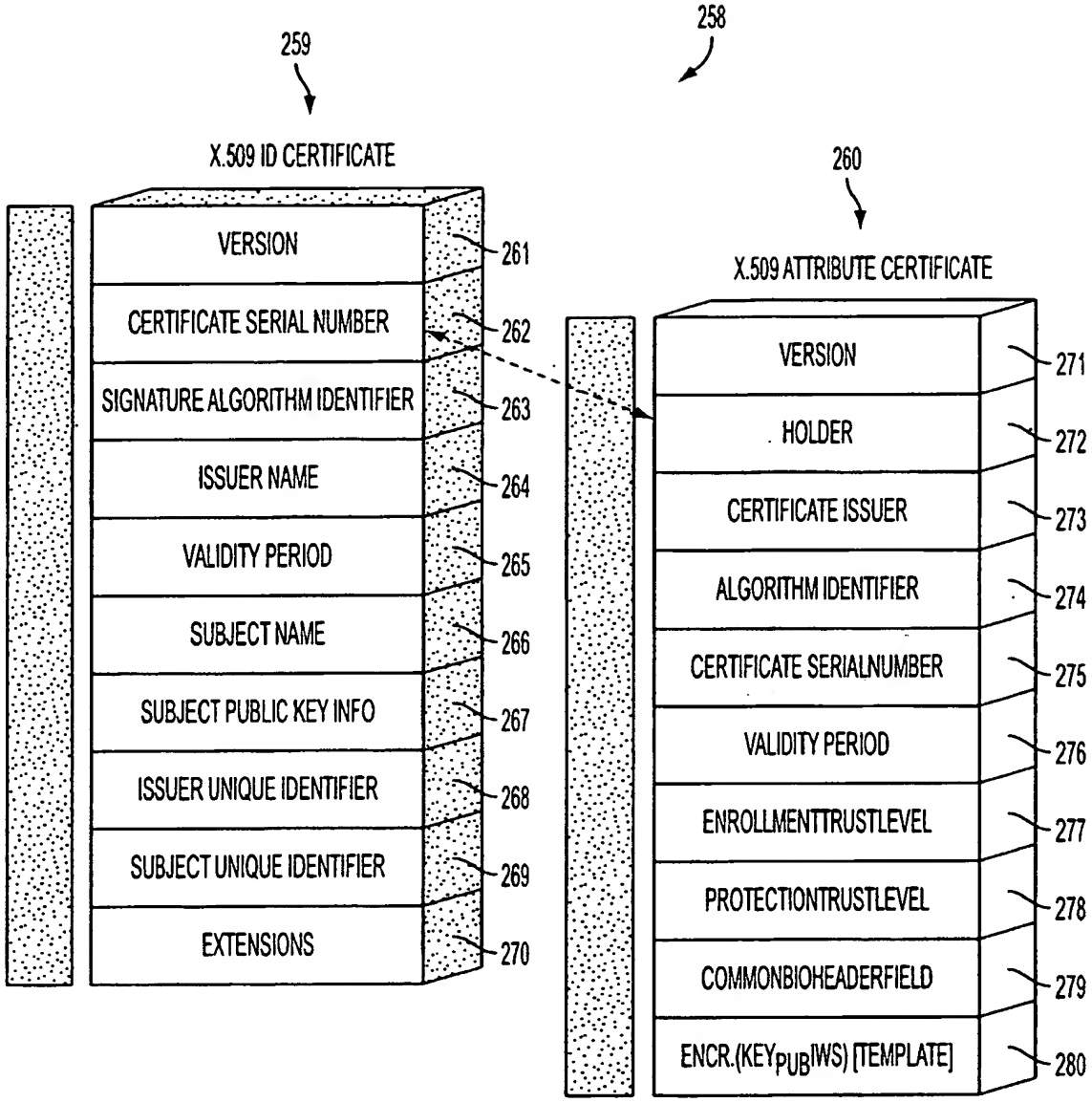


FIG. 8

BNSDOCID: <WO_____03007538A1_I_>

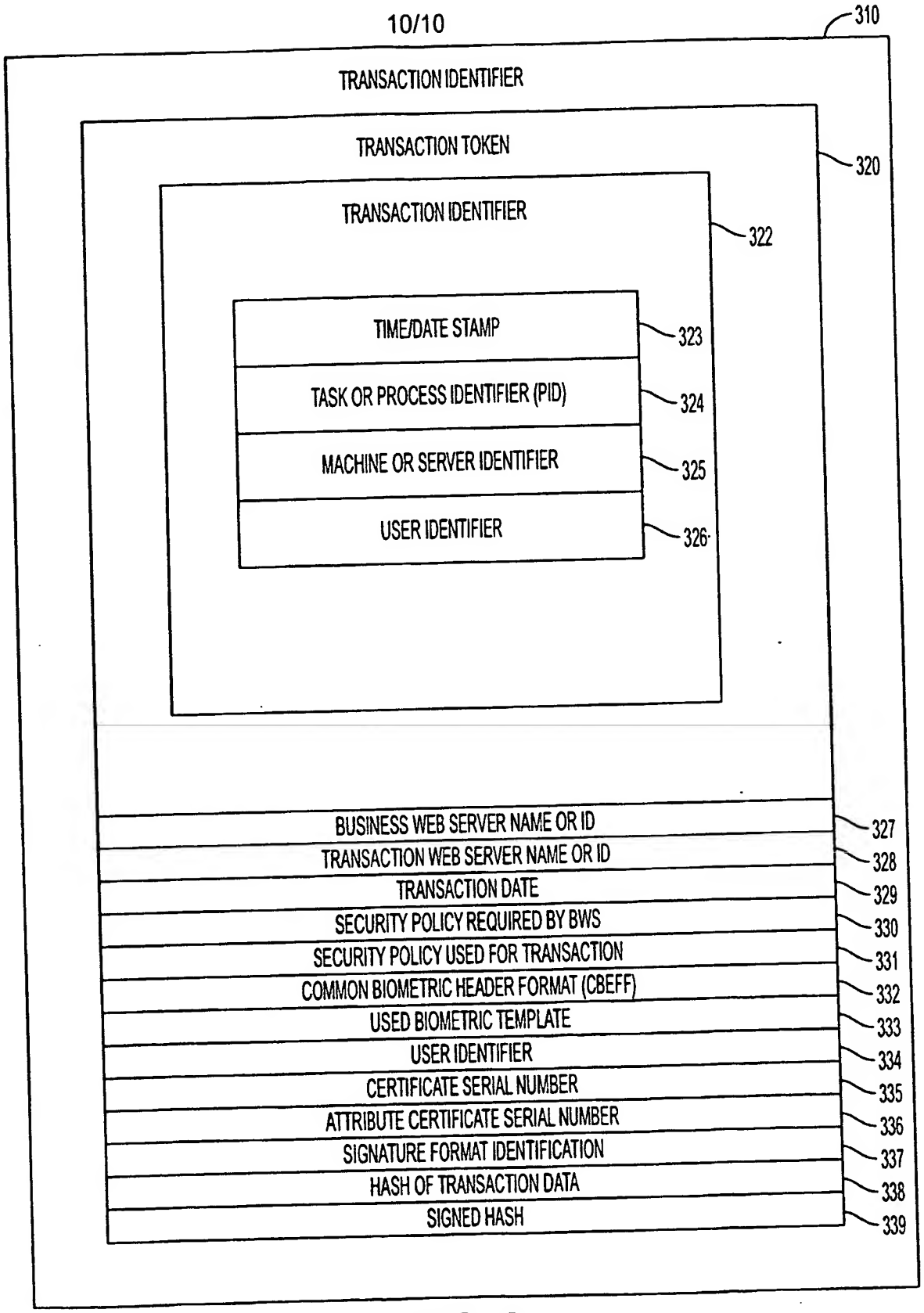


FIG. 9

BNSDOCID: <WO 03007538A1 | >

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/23237

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L9/00
US CL : 713/168

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/168; 705/26,27,35,39,41,44,64,65,67; 709/225,227,229; 379/142.05; 902/25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Microsoft Computer Dictionary Fifth Edition,

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East: authentication, transaction, server, biometric, wireless, X.509v3, interface, router, internet, challenge/response

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,047,268 A (Bartoli et al.) 04 April 2000 (04.04.2000) column 3 lines 8-10, 65-67; column 4 lines 1-6,42-45, 62-64; column 5 lines 57-65; column 6 lines 17-24; column 7 lines 35-43.	1-4,7,8,13-17,28,30,32 --- 5,18-20,22-24
Y	US 6,016,476 A (Maes et al.) 18 January 2000 (18.01.2000), column 3 lines 17-22, 33-37, 42-45; column 5 lines 54-63	5,18,19,20,22-24
Y	US 6,175,922 B1 (Wang) 16 January 2001 (16.01.2001), column 18 lines 44-45	19,20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 October 2002 (16.10.2002)	06 DEC 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Christopher J. Brown Telephone No. 703-305-8023

Form PCT/ISA/210 (second sheet) (July 1998)

This Page Blank (uspto)